

IN THE UNITED STATES DISTRICT COURT
FOR SOUTHERN DISTRICT OF ALABAMA

IN THE MATTER OF THE SEARCH OF

[REDACTED], TO
SEIZE AND SEARCH OF: A MOBILE
DEVICE UTILIZED BY JAVIS DORTCH
NOW IN THE POSSESSION OF
[REDACTED] OR [REDACTED]
[REDACTED] MOBILE NUMBER AND IMEI
CURRENTLY UNKNOWN

Case No. 25-MJ- 17-N

FILED UNDER SEAL

AFFIDAVIT IN SUPPORT OF APPLICATIONS FOR SEIZURE AND SEARCH
WARRANTS

I, Christopher Horton, a Task Force Officer ("TFO") with the Federal Bureau of Investigation ("FBI"), being duly sworn, depose and state:

INTRODUCTION, AGENT BACKGROUND, AND PURPOSE OF AFFIDAVIT

1. This affidavit does not contain every fact discovered during my investigation. Rather, the affidavit includes only those facts necessary to establish probable cause to assert that evidence of a violation of 18 U.S.C. § 922 (o) (possession of a machine gun) is present. The information contained within the affidavit is based on my own investigation, training, and experience, as well as information imparted to me by other law enforcement officers involved in this investigation.

2. I am a certified Federal Task Force Officer currently employed by the Monroe County Sheriff's Office, Monroeville, Alabama and assigned to the FBI having been so employed since 2019, and assigned to FBI since 2023.

3. I graduated from what is now known as the Alabama Criminal Justice Training Center, where I earned my Alabama Peace Officers and Training Commission (APOST) certification. I am currently a Certified Law Enforcement Officer through the Alabama Peace

Officers and Training Commission. In addition, I had been assigned to the Alabama Drug Enforcement Task Force where I am currently and have been involved with numerous narcotics investigations. I have attended several classes involving illegal narcotics sale, transport, and drug familiarization. I have been trained in various criminal investigation techniques including crime scene analysis, cell phone and digital device analysis and extractions.

4. As a TFO, my primary duties are to investigate violations of Title 18 of the United States Code. In this capacity, I received specialized training regarding the investigation and enforcement of Federal criminal violations. I am an investigative law enforcement officer of the United States within the meaning of Section 2510(7) of Title 18 United States Code, and I am empowered by law to conduct investigations and to make arrests for the offenses enumerated in Section 2516 of Title 18 United States Code. I have received training and experience in interviewing and interrogation techniques, surveillance techniques, arrest procedures, search and seizure, and asset forfeiture. I have also been involved in firearms, gang, and drug investigations, including the possession with intent to distribute and distribution of controlled substances, and conspiracies and offenses. I am also familiar with federal firearms violations and machine gun conversion devices commonly referred to as Glock switches.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that a violation 18 U.S.C. § 922(o) has been committed Jarvis Dortch (“Dortch”). There is also probable cause to search the premises described in Attachment A, and further described below, to locate and seize a mobile device (“the subject phone”) further described below. The subject phone is evidence, an instrumentality, contraband, and/or fruit of the above-referenced crimes, as further described in Attachment B. Attachments A and B are incorporated by reference.

APPLICABLE LAW

6. The investigation concerns alleged violation of 18 U.S.C. § 922 (o), relating to the possession of a machine gun. Section 922(o) states, “Except as provided in paragraph (2), it shall be unlawful for any person to transfer or possess a machinegun. (2) This subsection does not apply with respect to-- (A) a transfer to or by, or possession by or under the authority of, the United States or any department or agency thereof or a State, or a department, agency, or political subdivision thereof; or (B) any lawful transfer or lawful possession of a machinegun that was lawfully possessed before the date this subsection takes effect.” 18 U.S.C. § 922(o).

PROBABLE CAUSE

7. In October 2024, Dortch was indicted by the Grand Jury for the Southern District of Alabama. The Indictment alleges that on or about November 9, 2023, Dortch did knowingly possess a machinegun, namely, a Glock, model 17 9mm firearm, serial number BEPP950, equipped with a machinegun-conversion device, commonly referred to as a “Glock switch.” (Doc. 1, *United States of America v. Javis Dortch*, Case Number: 24-CR-00183-KD , pending in the United States District Court for the Southern District of Alabama).

8. The circumstances of that offense are as follows: In November 2023, during the course of a traffic stop, law enforcement located a firearm equipped with a machinegun conversion device or “Glock switch” on Dortch’s person. In a post-Miranda statement made to law enforcement, Dortch stated that he got the firearm with the switch from another individual but did not name that individual.

9. As the TFO assisting with this investigation, once the indictment was returned, I began efforts to locate Dortch to arrest him on the pending federal warrant.

10. Sometime in December 2024, Dortch or his family became aware of the pending

federal warrant.

11. On or about December 21, 2024, Dortch's stepfather, [REDACTED] ([REDACTED]) contacted me by telephone to discuss the pending federal charge and to make arrangements for Dortch to self surrender.

12. We agreed that Dortch would turn himself in at the Monroe County Sheriff's Office on December 31, 2024. [REDACTED] indicated he would communicate this arrangement to his wife, [REDACTED], and to their son, Javis Dortch.

13. On or about December 22, 2024, I spoke with [REDACTED] again who advised that Javis Dortch was aware of the arrangement and would turn himself in on December 31, 2024, as agreed.

14. On December 25, 2024, a deputy with the Monroe County Sheriff's Office observed a red Nissan Altima, license plate [REDACTED] (the Altima) operated by Dortch. The deputy was familiar with Dortch and recognized him in the driver's seat. The deputy was also aware that Dortch had active warrants but was not aware of any of the arrangements made for Dortch to turn himself in.

15. The deputy began a traffic stop on the Altima utilizing his emergency lights. However, rather than stopping, Dortch fled from the deputy and rapidly accelerated to speeds in excess of 75 mph on roads with speed limits of 25-35 mph. Ultimately, Dortch fled to his residence at [REDACTED] ("the residence and/or subject premises"). Dortch exited the vehicle, ran through the front door of the residence and out the back door. Dortch then fled into the wooded area near the residence.

16. Deputies searched the woods but did not find Dortch. When they returned to the residence, [REDACTED] told deputies he was able to get Dortch to return to the residence.

Deputies took Dortch into custody.

17. Dortch is 21 years old and lives at the residence with his mother and stepfather, [REDACTED].

[REDACTED] and [REDACTED]. All live at the subject premises.

18. When Dortch was taken into custody, no mobile devices or firearms were found on his person or in the vehicle. As most individuals keep phones on their person or in their immediate vicinity/access, this suggests that when he fled through the residence he disposed of the phone near or within that residence.

19. A few days after Dortch's arrest, Dortch's stepfather, [REDACTED], contacted me by phone and stated that he [REDACTED] was in possession of Dortch's phone and would provide it to me.

20. [REDACTED] also indicated that the phone contained information pertaining to the firearm and machinegun conversion device listed in the federal indictment.

21. In later conversations, when attempting to make arrangements to obtain the phone from [REDACTED] [REDACTED] advised that he no longer wished to provide Dortch's phone to me.

22. [REDACTED] did not indicate that he no longer has the phone, but stated that he and Dortch's mother would hold onto the phone until an attorney could review it.

23. Dortch was arrested on state charges and appeared in federal court in January 2025. He has been arraigned on the federal indictment and is in federal custody.

24. On December 31, 2024, I interviewed Dortch at the Monroe County Detention Center. I advised Dortch of his *Miranda* rights and he waived those rights and made a statement to me. During our conversation, Dortch stated that he received the firearm with the Glock switch that he possessed on or about November 9, 2023 from a specific individual whose nickname and

given name are known to me. Dortch stated that the subject phone contained receipts or texts messages related to his receipt of the firearm equipped with the switch from that individual. Dortch also stated that the subject phone was in the custody of his parents, [REDACTED] and [REDACTED].

25. Dortch's driver's license lists the residence as his address. Dortch provided the subject premises' address when he was booked into custody on December 25, 2024.

26. Both [REDACTED] and [REDACTED] driver's licenses and vehicle registrations list the subject premises as their address.

27. At the time of Dortch's arrest on December 25, 2024, he was operating an Altima registered to [REDACTED].

28. I am not aware of any other locations where [REDACTED] or [REDACTED] reside.

29. Since December 25, 2024, I have driven by the subject premises on several occasions and have observed vehicles registered to [REDACTED] and [REDACTED] at the residence.

30. As a mobile device is a small handheld device, it may be easily concealed on a person, within a home, or within a vehicle.

31. While [REDACTED] has confirmed that he has custody of Dortch's phone, details concerning the phone such as type of device, phone number, or IMEI are unknown to me. Dortch has also admitted that the phone in his [REDACTED] and/or [REDACTED]'s possession belongs to him.

32. Those executing the search warrant will make reasonable efforts to ensure seizure of only the phone belonging to Dortch and not other phones on the subject premises if law enforcement is able to determine ownership and control of phones belonging to others who may be on the subject premises.

TECHNICAL TERMS

33. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone, or mobile device) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable

storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- c. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.
- d. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a

keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

34. Based on my training, experience, and research, I know that the mobile device may have capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

35. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

36. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Subject Phone was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Subject Phone because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a

- file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
 - c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
 - d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
 - e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

37. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the Subject Phone consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many

parts of the Subject Phone to human inspection in order to determine whether it is evidence described by the warrant.

38. The warrant I am applying for would permit law enforcement to obtain from certain individuals the display of physical biometric characteristics (such as fingerprint, thumbprint, or facial characteristics) in order to unlock devices subject to search and seizure pursuant to this warrant. I seek this authority based on the following:

- a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners and facial recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.
- b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

- c. If a device is equipped with a facial recognition feature, a user may enable the ability to unlock the device through his or her face. For example, Apple offers a facial recognition feature called "Face ID." During the Face ID registration process, the user holds the device in front of his or her face. The device's camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Face ID.
- d. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.
- e. The passcode or password that would unlock the Subject Phone subject to search under this warrant is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the Subject Phone, making the use of biometric features necessary to the execution of the search authorized by this warrant.
- f. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such

features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when (1) more than 48 hours has elapsed since the device was last unlocked or (2) when the device has not been unlocked using a fingerprint for 4 hours *and* the passcode or password has not been entered in the last 156 hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

- g. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. It will likely be necessary for law enforcement to have the ability to require Dortch, reasonably believed by law enforcement to be a user of the Subject Phone, to unlock the Subject Phone using biometric features in the same manner as discussed above.
- h. Due to the foregoing, if law enforcement personnel encounter a device that is subject to search and seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, the warrant I am applying for would permit law enforcement personnel to (1) press or swipe the fingers (including thumbs) of Dortch, reasonably believed by law enforcement to be a user of the Subject Phone, to the fingerprint scanner of the Subject Phone (if any); (2) hold the Subject Phone in front of Dortch's face and activate the facial recognition feature

(if any), for the purpose of attempting to unlock the Subject Phone in order to search its contents as authorized by this warrant

IDENTIFICATION OF THE PREMISES TO BE SEARCHED
AND THE PROPERTY TO BE SEIZED

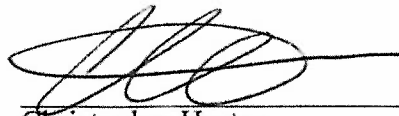
39. The property to be searched is [REDACTED] (the "Subject Premises"), including all buildings, outbuildings, vehicles, containers, trailers, or areas at Subject Premises where a cell phone could be reasonably stored. Agents have identified the Subject Premises as a property at which Dortch, [REDACTED], and [REDACTED] reside.

40. Agents seek authorization to enter and search the Subject Premises to locate and seize Dortch's mobile device, which I have probable cause to believe contains evidence of the above-described offense.

CONCLUSION


41. Based on the foregoing, I believe that there is probable cause to enter and search the Subject Premises to locate and seize Dortch's mobile device. There is also probable cause for a search warrant authorizing the seizure and examination of the Subject Phone described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



Christopher Horton
Task Force Officer
Federal Bureau of Investigation

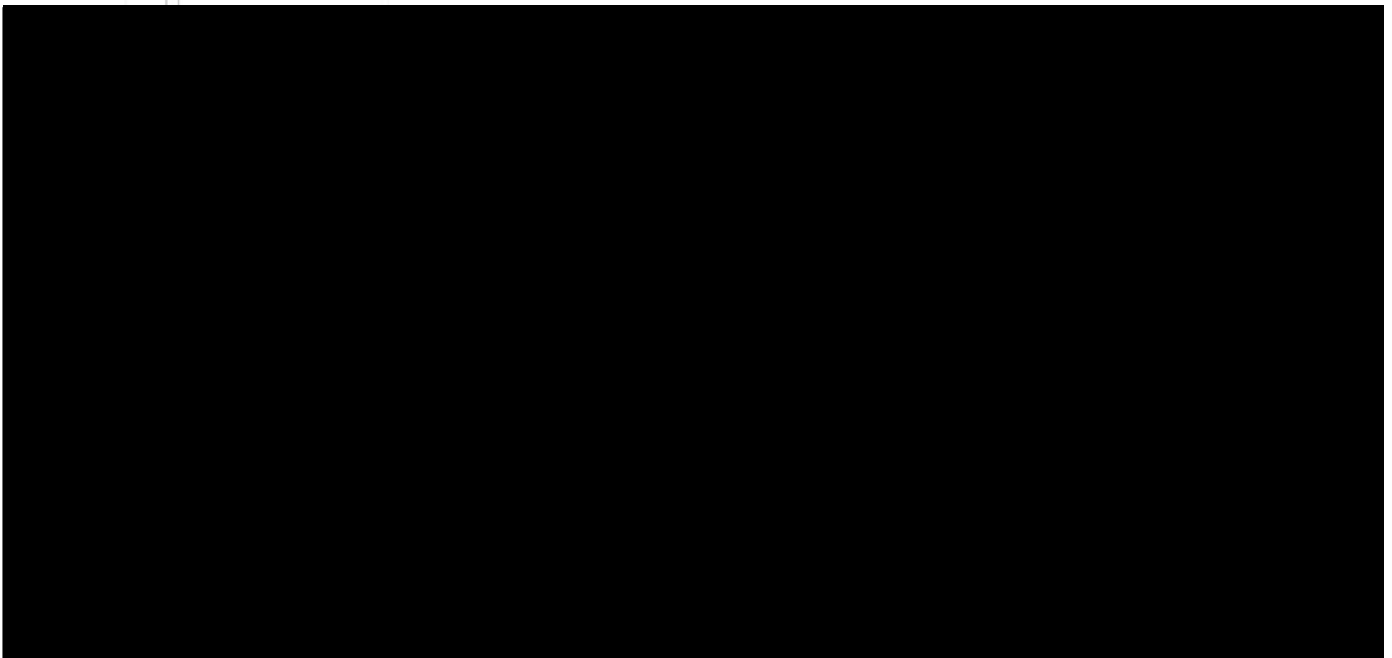
THE ABOVE AGENT HAD ATTESTED
TO THIS AFFIDAVIT PURSUANT TO
FED. R. CRIM. P. 4.1(b)(2)(B) THIS *24*
DAY OF JANUARY 2025.


KATHERINE P. NELSON
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

The property to be searched is [REDACTED] (the “Subject Premises”), including all buildings, outbuildings, vehicles, containers, trailers, or areas at the Subject Premises, which agents have identified as a family residence, and listed address Jarvis Dortch. Agents may also search the persons of [REDACTED] and [REDACTED] to locate the subject phone. A photograph of the Subject Premises appears below:



This warrant authorizes agents to enter and search the Subject Premises to locate and seize (1) the subject phone, a mobile device utilized or possessed by Jarvis Dortch. This warrant also authorizes the forensic examination of the subject phone for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

Particular Things to be Seized

The property to be seized is: (1) the Subject Phone, which constitutes evidence, fruits, and instrumentalities of violations of 18 U.S.C. §922(o) (illegal possession of a machinegun) by Dortch. The Subject Phone is believed to be located and stored at the Subject Premises.

This warrant also authorizes a search of all records on the Subject Phone described in Attachment A that relate to 18 U.S.C. §922(o) (illegal possession of a machinegun) and involve Dortch since September 9, 2023 (two months prior to Dortch's possession of the illegal machinegun as alleged in the indictment):

- a. communications regarding a machinegun conversion device and/or the firearm Dortch possessed on or about November 9, 2023
- b. any information related to the source of the machinegun conversion device
- c. any records related Dortch obtaining or paying for the machinegun conversion device
- d. Searches related to machinegun conversion devices /Glock switches, including how they function

Evidence of user attribution showing who used or owned the Subject Phone at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

During the execution of the search of the Subject Phone described in Attachment A, law

enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of Dortch, who is reasonably believed by law enforcement to be a user of the Subject Phone, to the fingerprint scanner of the Subject Phone (if any); (2) hold the Subject Phone in front of Dortch's face and activate the facial recognition feature (if any), for the purpose of attempting to unlock the Subject Phone in order to search their contents as authorized by this warrant.